



(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 098 267 A1

(12)

DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
09.05.2001 Bulletin 2001/19

(51) Int Cl.7: G06K 19/073

(21) Numéro de dépôt: 00403014.4

(22) Date de dépôt: 30.10.2000

(84) Etats contractants désignés:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU

MC NL PT SE

Etats d'extension désignés:

AL LT LV MK RO SI

(30) Priorité: 02.11.1999 FR 9913664

(71) Demandeur: SAGEM S.A.
75016 Paris (FR)

(72) Inventeurs:

• Chabanne, Hervé
78200 Mantes la Jolie (FR)
• Tissot, Nicolas
95240 Cormeilles en Parisis (FR)

(74) Mandataire: Gorrée, Jean-Michel
Cabinet Plasseraud,
84, rue d'Amsterdam
75440 Paris Cédex 09 (FR)

(54) Procédé pour assurer l'inviolabilité d'un micromodule de carte à puce contre une analyse de sa consommation de courant et micromodule agence pour sa mise en œuvre

(57) Pour assurer l'inviolabilité d'un microcircuit (2) de carte à puce contre une analyse du courant électrique qu'il consomme, on maximise la consommation électrique du microcircuit grâce à des moyens d'alimentation tampon inclus dans le micromodule, dans la ligne d'alimentation du microcircuit ; la fonction d'alimentation

tampon est obtenue en alimentant le microcircuit (2) à travers au moins deux condensateurs (8₁, 8₂) commutés, alternativement et en opposition l'un par rapport à l'autre, entre l'alimentation électrique (V_{cc}) pour qu'ils se chargent et la borne d'alimentation du microcircuit (2) pour qu'ils se déchargent dans celui-ci en l'alimentant électriquement.

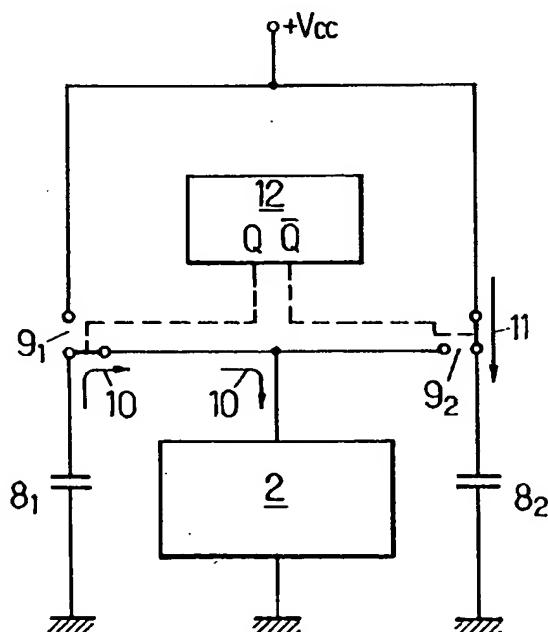


FIG.3.

Description

[0001] La présente invention concerne des perfectionnements apportés à la protection des cartes à puce contre les fraudes et plus particulièrement elle vise des perfectionnements destinés à assurer l'inviolabilité d'un micromodule de carte à puce contre une analyse de sa consommation de courant.

[0002] On rappellera tout d'abord que le micromodule est l'ensemble constitué par un microcircuit (ou puce), un réseau de contacts ou vignette disposé autour du microcircuit et à distance de celui-ci, et des fils fins reliant le microcircuit aux contacts, une résine enrobant le microcircuit et les fils et supportant les contacts en surface.

[0003] L'intensité du courant électrique consommé par un micromodule de carte à puce en cours de fonctionnement varie en fonction des valeurs traitées par le microcircuit contenu dans le micromodule.

[0004] Or l'énergie électrique nécessitée pour le fonctionnement de la carte à puce est fournie par la machine avec laquelle la carte coopère, autrement dit l'alimentation électrique est extérieure à la carte.

[0005] Il est donc possible, en détectant de façon continue l'intensité instantanée du courant nécessaire par la carte en fonctionnement, d'en déduire des informations sur les données traitées par la carte, et notamment, par exemple, d'en déduire un code secret.

[0006] Pour tenter d'éviter qu'une telle détection d'informations puisse être effectuée à partir du courant électrique consommé par le micromodule en fonctionnement, il est connu de modifier par un artifice le courant consommé par la carte, par exemple en lui ajoutant des valeurs aléatoires fournies par un générateur de signaux aléatoires.

[0007] L'inconvénient majeur de ces technologies connues est de nécessiter des moyens électroniques importants qui se traduisent par l'obligation d'ajouter, dans le microcircuit, un dispositif spécifique dédié au brouillage de la consommation de courant du microcircuit. Or la production d'un microcircuit nouveau est une opération qui, même lorsqu'il s'agit d'une modification effectuée sur un circuit préexistant, est complexe et très onéreuse, aussi bien pour la mise au point du nouveau circuit lui-même que pour la réalisation des outils de production.

[0008] L'invention a pour but de proposer des moyens simples et donc peu encombrants pour empêcher la détection de la valeur exacte de la consommation instantanée du micromodule.

[0009] A ces fins, selon un premier de ses aspects, l'invention propose un procédé pour assurer l'inviolabilité d'un micromodule de carte à puce contre une analyse du courant électrique consommé par le microcircuit contenu dans le micromodule au cours de son fonctionnement, lequel procédé se caractérise, selon l'invention, en ce qu'on maximise la consommation électrique du microcircuit grâce à des moyens d'alimentation tampon inclus dans le micromodule, dans la ligne d'alimen-

tation du microcircuit.

[0010] Dans un premier mode de mise en oeuvre du procédé, on dispose les moyens tampon au sein du microcircuit. Certes, cette manière de procéder entraîne une modification du microcircuit initial. Toutefois il ne s'agit, là, que d'une modification minime, d'une part, parce que le nombre des composants électroniques à mettre en oeuvre pour assurer la fonction d'alimentation tampon est relativement faible et donc conduit à un volume d'implantation restreint et, d'autre part, parce qu'un microcircuit tel que ceux employés dans les cartes à puce conserve des circuits et/ou composants non exploités pour l'application prévue et qui peuvent donc être récupérés pour assurer la fonction envisagée d'alimentation tampon.

[0011] Dans un second mode de mise en oeuvre, qui est préféré, du procédé, on dispose les moyens tampon entre le microcircuit et la vignette formée par l'ensemble des contacts du micromodule. Ce mode de mise en oeuvre est préféré car il est moins contraignant que le précédent. Les composants nécessaires à la fonction d'alimentation tampon peuvent alors être mis en oeuvre sous forme d'un microcircuit additionnel, de très petite dimension eu égard au relativement faible nombre des composants utilisés, qui peut trouver place dans l'espace restreint entre la vignette et le microcircuit principal. Le mode de mise en oeuvre préféré n'entraîne aucune modification du microcircuit principal et la mise en place du microcircuit additionnel est assurée par l'assembleur qui produit le micromodule.

[0012] De façon préférée, on assure la fonction d'alimentation tampon en alimentant le microcircuit à travers au moins deux condensateurs commutés, alternativement et en opposition l'un par rapport à l'autre, entre l'alimentation électrique pour qu'ils se chargent et la borne d'alimentation du microcircuit pour qu'ils se déchargent dans celui-ci en l'alimentant électriquement. Le nombre des composants nécessités par un tel processus d'alimentation par condensateurs commutés reste relativement peu élevé et le type des composants utilisés (essentiellement, d'une part, des condensateurs et, d'autre part, des interrupteurs réalisés sous forme de transistors utilisés en commutation) sont les composants couramment mis en oeuvre dans les intégrations à haute densité.

[0013] Le procédé conforme à l'invention faisant recours à la commutation séquentielle alternée de deux condensateurs procure un brouillage significatif du courant d'alimentation. Cependant la charge résiduelle du condensateur qui vient d'alimenter le micromodule et qui va être commutée sur le circuit de recharge demeure, encore, représentative du fonctionnement antérieur du microcircuit, et une information pourrait en être déduite concernant les données traitées par le microcircuit. Pour écarter, là aussi, cet inconvénient, un résultat d'une qualité encore accrue est obtenu en effectuant une décharge plus complète (au moins jusqu'à une valeur minimale préétablie) du condensateur qui vient

d'assurer l'alimentation du microcircuit, avant qu'il soit commuté en position de recharge : ainsi, la charge résiduelle, si elle existe, ne peut plus traduire le fonctionnement du microcircuit. A cet effet, selon cette mise en œuvre préférée du procédé de l'invention, on assure la fonction d'alimentation électrique tampon en alimentant le microcircuit à travers au moins trois condensateurs commutés cycliquement de manière que, simultanément :

- un premier condensateur, précédemment chargé, alimente le microcircuit,
- un deuxième condensateur, qui précédemment alimentait le microcircuit, est mis en court-circuit pour être plus déchargé,
- et un troisième condensateur, précédemment mis en court-circuit, est connecté à l'alimentation en vue d'être chargé,

ces étapes étant séquentiellement renouvelées avec permutation cyclique des condensateurs.

[0014] Selon un second de ses aspects, l'invention propose un micromodule de carte à puce agencé pour être inviolable contre une analyse du courant électrique qu'il consomme en fonctionnement, ce micromodule comprenant un microcircuit, une vignette constituée des contacts, et notamment un contact d'alimentation électrique, propres à la connexion avec un appareil de traitement, des fils reliant respectivement lesdits contacts au microcircuit, lequel micromodule, étant agencé selon l'invention, se caractérise en ce qu'il comprend en outre, fonctionnellement interposés entre le susdit contact d'alimentation de la vignette et le microcircuit, des moyens d'alimentation tampon propres à maximiser la consommation électrique du microcircuit au cours de son fonctionnement.

[0015] Dans un mode de réalisation possible, lesdits moyens d'alimentation tampon sont intégrés dans le microcircuit, immédiatement en aval de la borne d'alimentation de celui-ci.

[0016] Dans un autre mode de réalisation, qui est préféré, lesdits moyens d'alimentation tampon sont réalisés sous forme d'un microcircuit annexe indépendant disposé dans un emplacement de la zone intermédiaire séparant la vignette et le microcircuit principal, ledit microcircuit annexe possédant une entrée raccordée au contact d'alimentation de la vignette et une sortie raccordée à la borne d'alimentation du microcircuit principal.

[0017] De façon pratique, les moyens d'alimentation tampon sont du type à condensateurs commutés et comprennent

- au moins deux condensateurs ayant une borne connectée à la masse,
- des moyens sélecteurs associés à chaque condensateur, qui sont connectés à l'autre borne de chaque condensateur et qui sont propres à raccorder

celle-ci, sélectivement, au moins au contact d'alimentation ou au microcircuit,

- et des moyens de commande associés aux moyens sélecteurs pour commander ceux-ci de manière cyclique telle que, simultanément, un des condensateurs soit connecté au contact d'alimentation pour être chargé tandis qu'un autre condensateur est connecté au microcircuit pour alimenter celui-ci, puis inversement.

10

[0018] Dans un exemple de mise en œuvre simple, mais déjà efficace, les moyens d'alimentation tampon comprennent deux condensateurs.

15

[0019] Dans un exemple de mise en œuvre préférée qui conduit à un brouillage amélioré (meilleure maximisation de la consommation en courant d'alimentation), les moyens d'alimentation tampon comprennent trois condensateurs, et les moyens de commande associés aux moyens sélecteurs sont propres à commander ceux-ci de manière cyclique telle que, simultanément, un des condensateurs, précédemment déchargé, soit connecté au contact d'alimentation pour être chargé, tandis qu'un autre condensateur, précédemment en charge, est connecté au microcircuit pour alimenter celui-ci, et tandis enfin que le dernier condensateur, qui alimentait précédemment le microcircuit, est connecté à la masse pour être mis en court-circuit en vue d'être déchargé.

25

[0020] Pour obtenir des séquences de commutation évitant des doubles liaisons même très brèves, il est souhaitable que les moyens sélecteurs associés à chaque condensateur comprennent des couples d'interrupteurs connectés, d'un côté, au condensateur et, de l'autre côté, au contact d'alimentation pour l'un et au microcircuit pour l'autre et que les moyens de commande soient propres à commander les couples d'interrupteurs de manière séquentielle propre à éviter les connexions interférentes sur le microcircuit.

30

[0021] L'invention sera mieux comprise à la lecture de la description détaillée qui suit de certains modes de réalisation donnés à titre d'exemples non limitatifs. Dans cette description, on se réfère aux dessins annexés sur lesquels :

45

- la figure 1 illustre schématiquement un micromodule agencé selon un premier mode de réalisation conformément à l'invention ;
- la figure 2 illustre schématiquement un micromodule agencé selon un second mode de réalisation, préféré, conformément à l'invention ;
- les figures 3 et 4 sont des schémas électriques d'un premier exemple de réalisation, simple, montré dans deux configurations fonctionnelles, respectivement ;
- la figure 5 est un schéma électrique d'une variante préférée du premier exemple de réalisation des figures 3 et 4 ;
- la figure 6 est un schéma électrique d'un exemple

- de réalisation d'un composant de commande inclus dans les circuits des figures 3 à 5 ;
- la figure 7 illustre, par trois diagrammes, des séquences impulsionnelles respectivement à l'entrée et aux sorties du composant de commande de la figure 6 ;
 - la figure 8 est un schéma électrique d'un second exemple de réalisation, préféré, conforme à l'invention ;
 - la figure 9 est un schéma électrique d'une variante de réalisation de certaines branches du circuit de la figure 8 ;
 - la figure 10 est un schéma électrique d'un exemple de réalisation d'un composant de commande inclus dans le circuit de la figure 8 ; et
 - la figure 11 illustre, par six diagrammes, des séquences impulsionnelles en six positions du circuit de la figure 8, respectivement.

[0022] En se reportant tout d'abord aux figures 1 et 2, un micromodule 1 pour carte à puce ou analogue comprend essentiellement un microcircuit 2 (ou puce) - qui est un composant électronique à très haute intégration incluant en général au moins un microprocesseur - autour duquel est agencée une vignette 3 formée par un ensemble de contacts plats 4 ; des fils 5 relient le microcircuit 2 à chaque contact 4 ; le microcircuit 2 et les fils 5 sont enrobés dans une résine, à la surface de laquelle apparaissent les contacts 4.

[0023] Les contacts 4 sont propres à coopérer avec des contacts mobiles d'un appareil dans lequel la carte est introduite, et chaque contact 4 est affecté à une liaison spécifique pour l'échange de signaux électriques avec l'appareil : en particulier sont présents les contacts d'alimentation V_{cc} (l'alimentation électrique nécessaire au fonctionnement du micromodule est assurée par l'appareil), d'horloge H, de réinitialisation R, d'échange des données I/O ; la masse M est constituée par le reste de la surface métallique non affectée aux contacts spécifiques 5 formant la vignette 3 (pour plus de clarté, le contact de masse a été représenté en gris clair sur les figures 1 et 2).

[0024] Pour assurer l'inviolabilité du micromodule face à une fraude par analyse du courant électrique consommé par le microcircuit en fonctionnement, l'invention propose de maximiser, au moins dans une certaine mesure, la consommation électrique du microcircuit afin d'empêcher que les variations instantanées du courant reflètent les opérations fonctionnelles du microcircuit, et en particulier reflètent les signes (par exemple ceux d'un code secret) traités par le microcircuit.

[0025] Une telle fonction de maximisation de la consommation est obtenue grâce à des moyens d'alimentation tampon inclus dans le micromodule, dans la ligne d'alimentation du microcircuit ; elle ne met en oeuvre qu'un nombre réduit de composants et ces moyens peuvent alors être aisément intégrés dans le micromodule 1.

[0026] Dans un premier mode de réalisation illustré à la figure 1, les moyens d'alimentation tampon sont intégrés au microcircuit 2 (schématisation par le rectangle 6) au niveau de la borne d'alimentation du microcircuit et ils sont reliés directement au contact 5 d'alimentation V_{cc} . Les moyens d'alimentation tampon 6 constituent ainsi l'entrée d'alimentation électrique du microcircuit. Bien qu'une telle implantation entraîne une modification des microcircuits préexistants, l'aménagement demeure toutefois restreint si l'on exploite des circuits et/ou composants présents dans les microcircuits, mais non utilisés dans le cadre de leur application traditionnelle. Bien que cela n'apparaisse pas sur la figure 1 pour ne pas alourdir le dessin, les moyens de lissage 6 sont raccordés non seulement à l'alimentation V_{cc} , mais également à d'autres sources de signaux (notamment les signaux d'horloge H) et bien sûr à la masse M.

[0027] A la figure 2 est illustré un second mode de réalisation, qui est préféré, dans lequel les moyens d'alimentation tampon sont réalisés sous forme d'un microcircuit annexe 7, de très petites dimensions en raison du nombre réduit des composants, et propre à être disposé dans l'intervalle extrêmement restreint entre la vignette 3 et le microcircuit 2. Le microcircuit annexe 7 est relié par des fils au contact d'alimentation V_{cc} (le microcircuit principal 2 n'étant plus relié directement à ce contact), et est relié à la masse et à l'horloge directement par des fils propres et/ou à travers le microcircuit principal 2. Un tel mode de réalisation est préféré car il n'affecte en rien le microcircuit principal, et la mise en place du microcircuit annexe est effectuée au cours de la fabrication du micromodule.

[0028] Une mise en oeuvre simple de l'invention fait appel à des condensateurs commutés. Le microcircuit 2 n'est plus alimenté directement à partir du contact 4 d'alimentation V_{cc} , mais à partir de condensateurs qui sont cycliquement et alternativement rechargés : ainsi le courant délivré par l'alimentation V_{cc} n'est plus le reflet exact du courant instantané consommé par le microcircuit.

[0029] Aux figures 3 et 4 est représenté un schéma électrique illustrant un mode de réalisation simple des dispositions de l'invention. Deux condensateurs 8_1 , 8_2 sont reliés, par une de leurs bornes, à la masse. Leur autre borne est reliée au contact mobile d'un sélecteur 9_1 , 9_2 dont une borne est reliée à l'alimentation V_{cc} et l'autre borne est reliée au microcircuit 2 (borne d'entrée d'alimentation V_{cc} du microcircuit 2).

[0030] Dans la position fonctionnelle montrée à la figure 3, l'un des sélecteurs situé à gauche 9_1 relie le condensateur 8_1 correspondant au microcircuit : ayant été préalablement chargé, le condensateur 8_1 alimente le microcircuit 2 en se déchargeant dans celui-ci (flèches 10). Pendant ce temps, l'autre sélecteur 9_2 est dans une position reliant le condensateur correspondant 8_2 à l'alimentation V_{cc} : le condensateur 8_2 se charge (flèche 11).

[0031] Avant que le condensateur 8_1 soit trop déchar-

gé (autrement dit avant que sa tension soit descendue en dessous d'un seuil prédéterminé), les deux sélecteurs 9₁ et 9₂ sont inversés. Ainsi, tandis que c'est maintenant le condensateur 8₁ qui est relié à l'alimentation V_{cc} et qui se charge, le condensateur 8₂ est raccordé au microcircuit 2 qu'il alimente.

[0032] Des moyens de commande 12 assurent la commande synchrone et cyclique des sélecteurs 8₁ et 8₂ pour leur faire occuper leurs deux positions alternativement et en opposition l'un par rapport à l'autre. La durée de chaque cycle doit être suffisamment brève pour que la décharge du condensateur alimentant le microcircuit n'amène pas la tension en-dessous d'une valeur de seuil. Par exemple, la commutation est déterminée pour que la décharge du condensateur n'excède pas 20 % de sa pleine charge pour la consommation maximale du microcircuit.

[0033] Pour éviter des interruptions d'alimentation du microcircuit (basculement rigoureusement synchrone des deux sélecteurs) ou pour éviter des chevauchements d'alimentation (basculement désynchronisé des deux sélecteurs), il est préférable de remplacer chaque sélecteur 9 par deux interrupteurs 13 (du côté alimentation V_{cc}) et 14 (du côté microcircuit 2). Les interrupteurs sont alors commandés simultanément de façon croisée (interrupteurs 13₁, 14₂ ; interrupteurs 13₂, 14₁) comme illustré à la figure 5 ou individuellement avec des décalages. Cette solution technique offre en outre l'avantage, du point de vue de l'intégration, que chaque interrupteur est réalisé de façon simple par un transistor commandé par impulsions.

[0034] Les moyens de commande 12 peuvent, de façon très simple, être constitués par le signal d'horloge H et son complément \bar{H} . On peut aussi, comme illustré à la figure 6, mettre en oeuvre un compteur binaire (par exemple le circuit disponible dans le commerce sous la référence 74 HCT 193 E) déclenché par les fronts montants du signal d'horloge H et fournissant sur ses deux sorties Q et \bar{Q} des signaux en opposition de phase. A la figure 7, sont représentés les diagrammes illustrant le signal d'horloge H, le signal de sortie Q et le signal inversé \bar{Q} .

[0035] Bien que le montage à deux condensateurs commutés qui vient d'être décrit procure une relative maximisation de la consommation du microcircuit, le résultat obtenu peut, au moins pour certaines applications, se révéler insuffisant. En effet, le taux de décharge de chaque condensateur au moment de la commutation dépend de la consommation du microcircuit au cours du cycle correspondant. De ce fait ce taux de décharge (ou son corollaire le taux de charge résiduel) peut être détecté au cours du cycle de charge immédiatement consécutif et une information sur le fonctionnement du microcircuit peut en être déduite.

[0036] On propose donc, pour écarter cet inconvénient, que chaque condensateur, avant d'être rechargeé (et donc connecté à l'alimentation V_{cc}), soit encore plus déchargé, notamment jusqu'à une valeur de seuil pré-

déterminée. A cet effet, on a recours à un mode de réalisation à trois condensateurs commutés cycliquement comme illustré à la figure 8. Chaque branche est constituée de la même manière que chaque branche du montage de la figure 5, avec en outre un interrupteur additionnel 15 disposé en parallèle sur chaque condensateur 13 pour commander la décharge additionnelle de celui-ci. Sur la figure 8, les composants de chaque branche sont désignés avec les mêmes références numériques que ceux correspondants de la figure 5, avec un indice i = 1, 2, 3 pour les branches respectives. Les moyens de commande 16 peuvent, comme illustré, comporter trois sorties C₀, C₁, C₂ raccordées chacune à trois interrupteurs (un par branche) de façon que chaque cycle assure simultanément les trois fonctions suivantes :

- un condensateur (8₁ sur la figure 8) est raccordé à l'entrée d'alimentation du microcircuit 2 et, ayant été préalablement chargé, il alimente celui-ci (flèches 10) ;
- un condensateur (8₂ sur la figure 8), qui alimentait précédemment le microcircuit 2, est court-circuité par l'interrupteur 15₂ fermé et est donc encore plus déchargé ;
- un condensateur (8₃ sur la figure 8), qui a été préalablement déchargé, est relié à l'alimentation V_{cc} pour être chargé.

[0037] Une prédétermination du seuil de décharge peut être obtenue en insérant un élément tel qu'une diode Zéner 17 entre chaque interrupteur de court-circuit 15 et la masse. La figure 9 illustre une branche ainsi agencée.

[0038] Les condensateurs 8 doivent avoir une capacité de l'ordre de la dizaine de nanofarads. Les diodes Zéner sont de type 4,3 V. Les interrupteurs commandés en tension doivent présenter une impédance aussi faible que possible en position passante. Compte tenu de l'impédance relativement élevée des diodes Zéner, chaque interrupteur de court-circuit 15 peut se limiter à un simple transistor de type NMOS, ce qui améliore l'efficacité.

[0039] Les moyens de commande 16 peuvent être constitués comme illustré à la figure 10 : un compteur binaire 18 (par exemple disponible dans le commerce sous la référence 74 HCT 193 E) reçoit sur son entrée les impulsions d'horloge H ; sa sortie inversée \bar{Q} est bouclée sur l'entrée de remise à zéro RAZ. Les deux sorties directe Q et inversée \bar{Q} sont reliées aux entrées respectives d'un décodeur binaire 19 (démultiplexage 2 pour 4) - par exemple du type disponible dans le commerce sous la référence 74 HCT 139 E) - dont les trois sorties délivrent des signaux cycliques C₀, C₁, C₂ servant à la commande cyclique des trois branches comme exposé ci-dessus.

[0040] A la figure 11, les diagrammes montrent successivement le signal d'horloge H appliqué à l'entrée du

compteur binaire 18, les deux signaux en opposition de phase Q et \bar{Q} présents aux deux sorties dudit compteur et appliqués aux entrées du décodeur 19, et les trois signaux C_0 , C_1 , C_2 commandant des triplets d'interrupteurs pour procurer l'alimentation cyclique du microcircuit 2.

[0041] Bien entendu, d'autres dispositions peuvent être mises en oeuvre sans sortir du cadre de l'invention. En particulier, le nombre des branches commutées cycliquement peut être accru, et être porté par exemple à quatre ou cinq, sachant que la maximisation de la consommation du micromodule (et donc la qualité du brouillage obtenue) est d'autant meilleure que le nombre de branches est accru.

[0042] On notera en définitive que l'invention conduit aux avantages suivants :

- la consommation de courant électrique mesurée sur la vignette ne reflète plus la consommation nécessaire à l'exécution des instructions sur le microcircuit ;
- la pose d'une résistance sur la vignette (nécessaire pour mesurer le courant consommé) est susceptible d'augmenter le temps de charge des condensateurs, et donc d'empêcher le fonctionnement normal du microcircuit, ce qui rend la carte à puce invalide temporairement ;
- la destruction du dispositif de l'invention annexé au microcircuit entraîne la destruction du micromodule : il reste alors des traces visibles puisque le micromodule est encastré dans un support en matière plastique (carte) ; la carte à puce peut alors être invalidée définitivement.

Revendications

1. Procédé pour assurer l'inviolabilité d'un micromodule de carte à puce contre une analyse du courant électrique consommé par le microcircuit contenu dans le micromodule au cours de son fonctionnement, caractérisé en ce qu'on maximise la consommation électrique du microcircuit grâce à des moyens d'alimentation tampon inclus dans le micromodule, dans la ligne d'alimentation du microcircuit.
2. Procédé selon la revendication 1, caractérisé en ce qu'on dispose les moyens d'alimentation tampon au sein du microcircuit.
3. Procédé selon la revendication 1, caractérisé en ce qu'on dispose les moyens d'alimentation tampon entre le microcircuit et la vignette formée par l'ensemble des contacts du micromodule.
4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'on assure la fonction d'alimentation tampon en alimentant le mi-

cro circuit à travers au moins deux condensateurs commutés, alternativement et en opposition l'un par rapport à l'autre, entre l'alimentation électrique pour qu'ils se chargent et la borne d'alimentation du microcircuit pour qu'ils se déchargent dans celui-ci en l'alimentant électriquement.

5. Procédé selon la revendication 4, caractérisé en ce qu'on assure la fonction d'alimentation tampon en alimentant le microcircuit à travers au moins trois condensateurs commutés cycliquement de manière que, simultanément :

- un premier condensateur, précédemment chargé, alimente le microcircuit,
- un deuxième condensateur, qui précédemment alimentait le microcircuit, est mis en court-circuit pour être plus déchargé,
- et un troisième condensateur, précédemment mis en court-circuit, est connecté à l'alimentation en vue d'être chargé,

ces étapes étant séquentiellement renouvelées avec permutation cyclique des condensateurs.

6. Micromodule de carte à puce agencé pour être inviolable contre une analyse du courant électrique qu'il consomme en fonctionnement, ce micromodule (1) comprenant un microcircuit (2), une vignette (3) constituée des contacts (4), et notamment un contact d'alimentation électrique V_{cc} , propres à la connexion avec un appareil de traitement, des fils (5) reliant respectivement lesdits contacts (4) au microcircuit (2),

caractérisé en ce qu'il comprend en outre, fonctionnellement interposés entre le susdit contact (4) d'alimentation V_{cc} de la vignette (3) et le microcircuit (2), des moyens (6, 7) d'alimentation tampon propres à maximiser le courant électrique consommé par le microcircuit au cours de son fonctionnement.

7. Micromodule selon la revendication 6, caractérisé en ce que lesdits moyens d'alimentation tampon (6) sont intégrés dans le microcircuit (2), immédiatement en aval de la borne d'alimentation de celui-ci.

8. Micromodule selon la revendication 6, caractérisé en ce que lesdits moyens d'alimentation tampon sont réalisés sous forme d'un microcircuit annexe indépendant (7) disposé dans un emplacement de la zone intermédiaire séparant la vignette (3) et le microcircuit principal (2), ledit microcircuit annexe (7) possédant une entrée raccordée au contact (4) d'alimentation V_{cc} de la vignette (3) et une sortie raccordée à la borne d'alimentation du microcircuit principal (2).

9. Micromodule selon l'une quelconque des revendications 6 à 8, caractérisé en ce que les moyens d'alimentation tampon (6, 7) sont du type à condensateurs (8) commutés et comprennent

5

- au moins deux condensateurs (8) ayant une borne connectée à la masse,
- des moyens sélecteurs (9 ; 13, 14, 15) associés à chaque condensateur, qui sont connectés à l'autre borne de chaque condensateur et qui sont propres à raccorder celle-ci, sélectivement, au moins à l'alimentation V_{cc} ou au microcircuit (2),
- et des moyens de commande (12, 16) associés aux moyens sélecteurs (9) pour commander ceux-ci de manière cyclique telle que, simultanément, un des condensateurs soit connecté à l'alimentation V_{cc} pour être chargé tandis qu'un autre condensateur est connecté au microcircuit (2) pour alimenter celui-ci, puis inversement.

10

15

20

10. Micromodule selon la revendication 9, caractérisé en ce que les moyens d'alimentation tampon comprennent deux condensateurs ($8_1, 8_2$).

25

11. Micromodule selon la revendication 9, caractérisé en ce que les moyens d'alimentation tampon comprennent trois condensateurs ($8_1, 8_2, 8_3$), et en ce que les moyens de commande (16) associés aux moyens sélecteurs ($13_1, 13_2, 13_3 ; 14_1, 14_2, 14_3 ; 15_1, 15_2, 15_3$) sont propres à commander ceux-ci de manière cyclique telle que, simultanément, un des condensateurs, précédemment déchargé, soit connecté au contact d'alimentation pour être chargé, tandis qu'un autre condensateur, précédemment en charge, soit connecté au microcircuit pour alimenter celui-ci, et tandis enfin que le dernier condensateur, qui alimentait précédemment le microcircuit, soit connecté à la masse pour être mis en court-circuit en vue d'être plus déchargé.

30

35

40

12. Micromodule selon l'une quelconque des revendications 9 à 11, caractérisé en ce que les moyens sélecteurs associés à chaque condensateur comprennent des couples d'interrupteurs ($13_i, 14_i$) connectés, d'un côté, au condensateur (8_i) et, de l'autre côté, à l'alimentation V_{cc} pour l'un et au microcircuit (2) pour l'autre et en ce que les moyens de commande (16) sont propres à commander les couples d'interrupteurs ($13_i, 14_i$) de manière séquentielle propre à éviter les connexions interférentes sur le microcircuit (2).

45

50

55

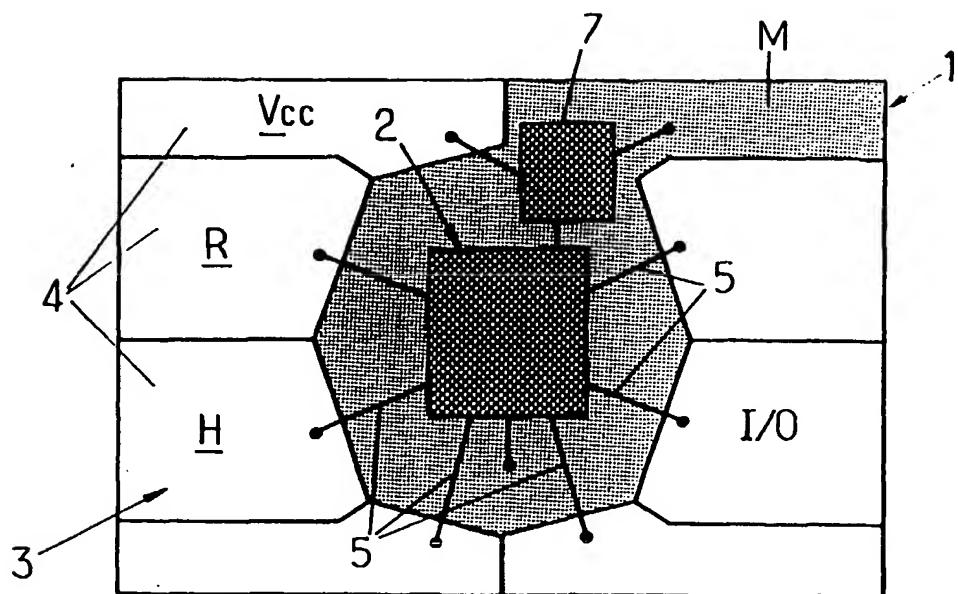


FIG.2

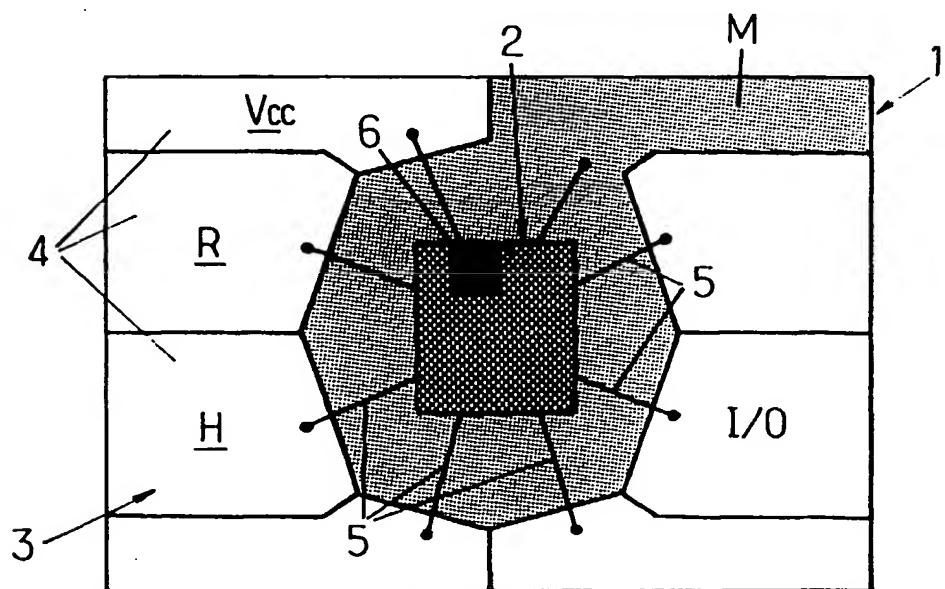


FIG.1.

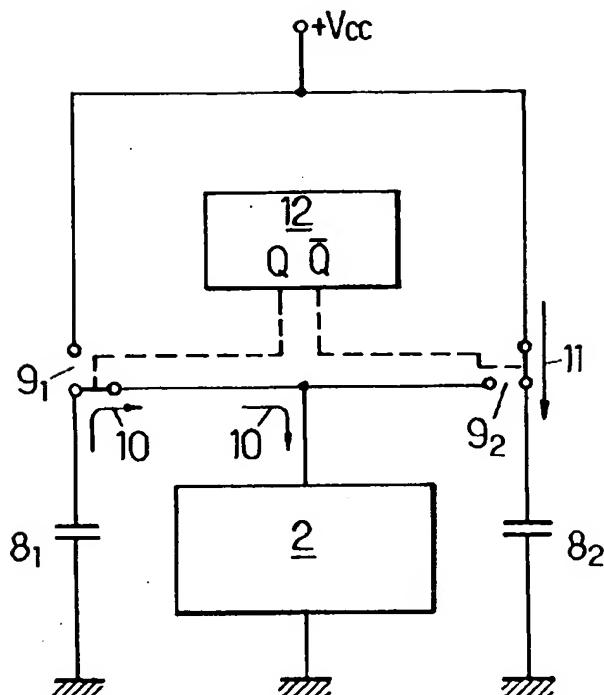


FIG.3.

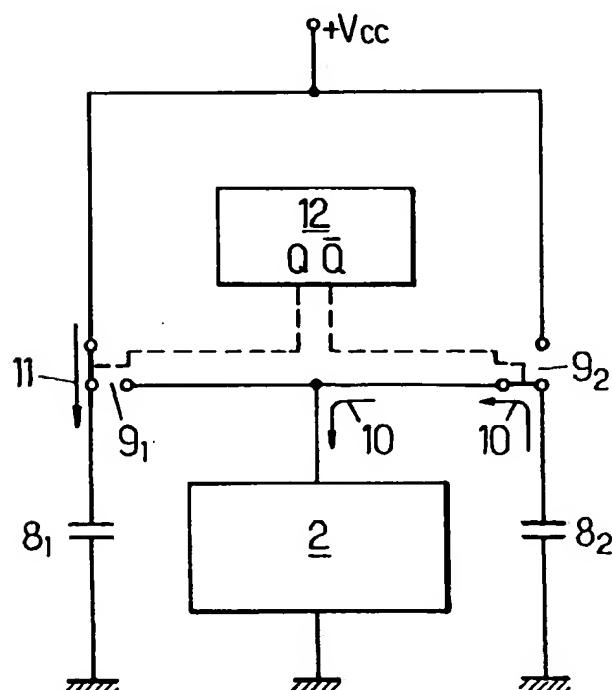


FIG.4.

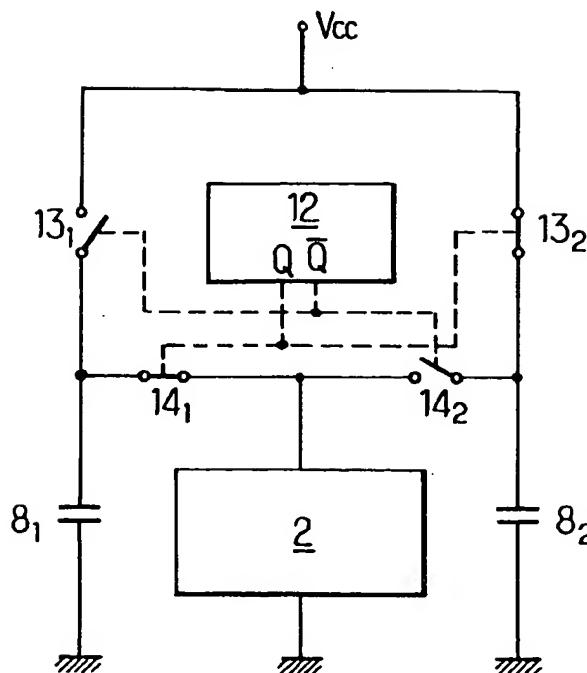


FIG. 5.

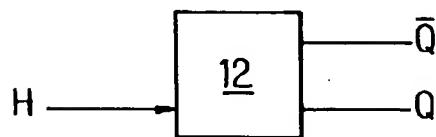


FIG. 6.

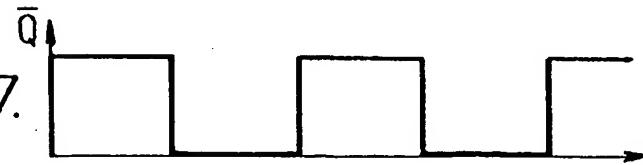
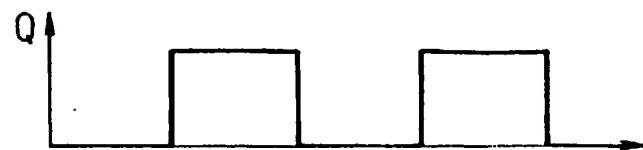
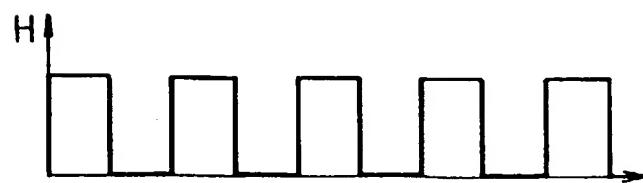


FIG. 7.

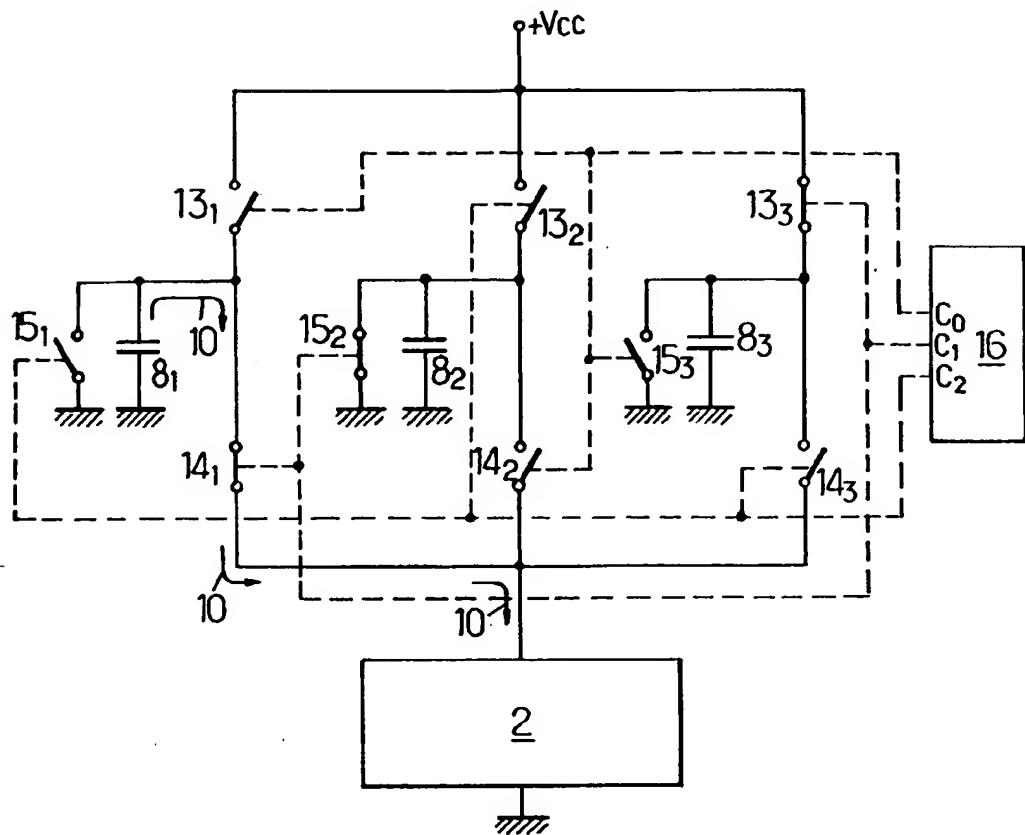


FIG. 8.

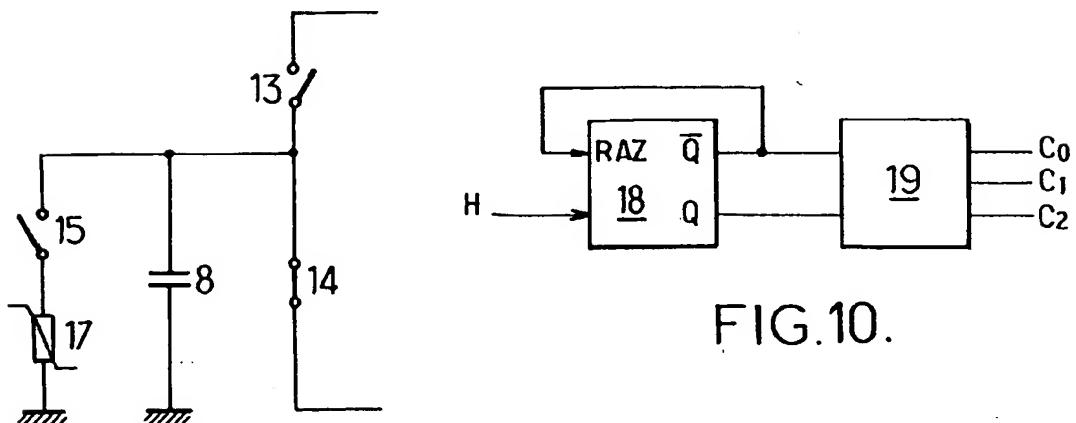


FIG. 10.

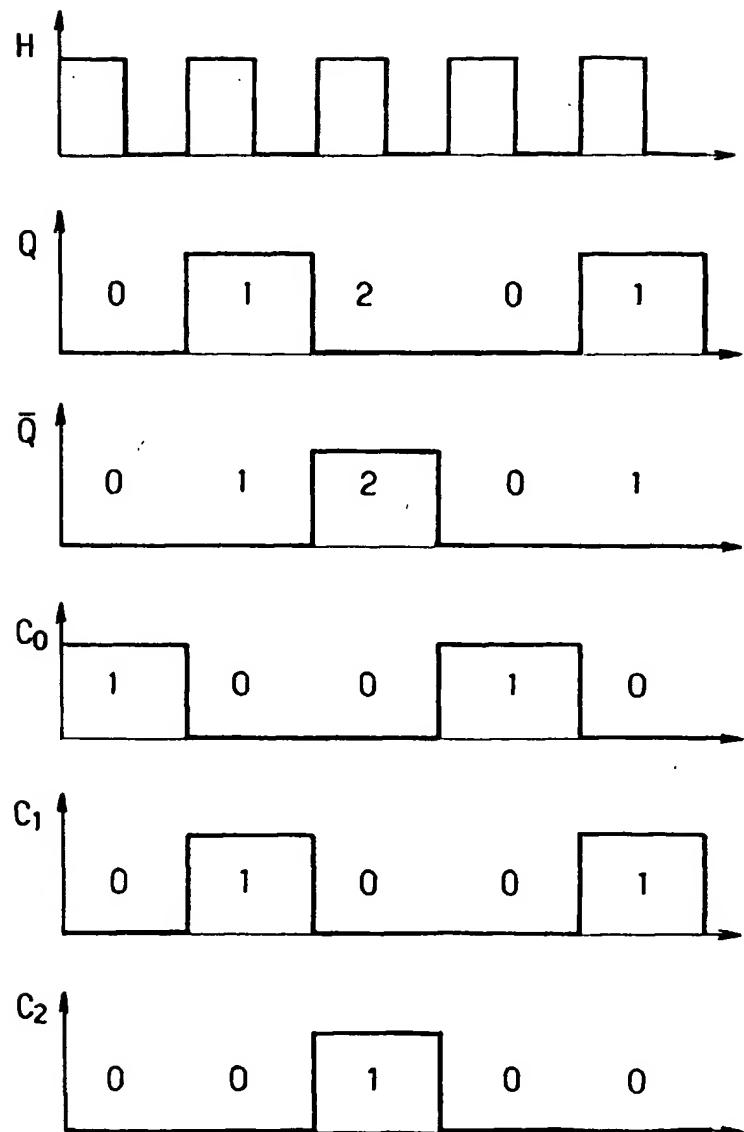


FIG.11.



Office européen
des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 00 40 3014

DOCUMENTS CONSIDERES COMME PERTINENTS									
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)						
A	FR 2 776 410 A (GEMPLUS CARD INT) 24 septembre 1999 (1999-09-24) * abrégé * * page 1 - page 6 * * figure 1 *	1-3,6-8	G06K19/073						
A	US 4 881 199 A (KOWALSKI JACEK) 14 novembre 1989 (1989-11-14) * colonne 2, ligne 7 - colonne 6, ligne 35 * * figures 1,2A *	1-3,6-8							
A	FR 2 774 492 A (SCHLUMBERGER IND SA) 6 août 1999 (1999-08-06) * abrégé * * page 1 - page 4 * * page 9, ligne 4 - ligne 29 *	1-3,6,7							
DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)									
G06K G11C G06F									
<p>Le présent rapport a été établi pour toutes les revendications</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;">Lieu de la recherche</td> <td style="width: 33%;">Date d'achèvement de la recherche</td> <td style="width: 33%;">Examinateur</td> </tr> <tr> <td>LA HAYE</td> <td>5 février 2001</td> <td>Jacobs, P</td> </tr> </table>				Lieu de la recherche	Date d'achèvement de la recherche	Examinateur	LA HAYE	5 février 2001	Jacobs, P
Lieu de la recherche	Date d'achèvement de la recherche	Examinateur							
LA HAYE	5 février 2001	Jacobs, P							
CATÉGORIE DES DOCUMENTS CITÉS		T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons S : membre de la même famille, document correspondant							
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrrière-plan technologique O : divulgarion non-écrite P : document intercalaire									

**ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE
RELATIF A LA DEMANDE DE BREVET EUROPEEN NO.**

EP 00 40 3014

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.

Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

05-02-2001

Document brevet cité au rapport de recherche		Date de publication		Membre(s) de la famille de brevet(s)		Date de publication
FR 2776410	A	24-09-1999		EP 1062633 A WO 9949416 A		27-12-2000 30-09-1999
US 4881199	A	14-11-1989		FR 2609831 A DE 3869158 A EP 0279712 A JP 2673945 B JP 63192146 A		22-07-1988 23-04-1992 24-08-1988 05-11-1997 09-08-1988
FR 2774492	A	06-08-1999		EP 1053531 A WO 9940538 A		22-11-2000 12-08-1999

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82